PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-004407**
(43)Date of publication of application : **14.01.1994**

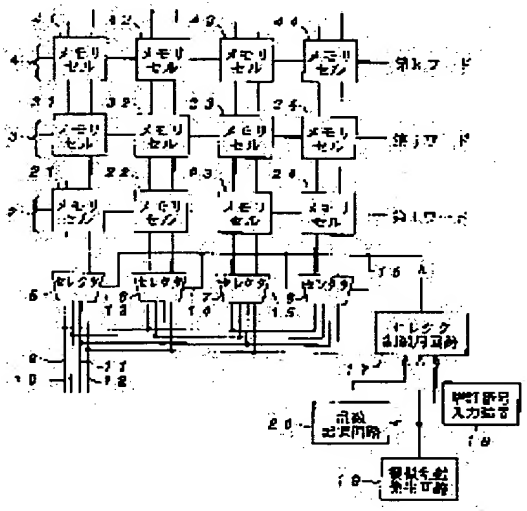
(51)Int.Cl. **G06F 12/14**
G06F 9/06

(21)Application number : **04-187474**
(22)Date of filing : **22.06.1992**

(71)Applicant : **NIPPON STEEL CORP**
(72)Inventor : **NISHIMURA SATOHIKO**

(54) DEVICE AND METHOD FOR STORING DATA

(57)Abstract:
PURPOSE: To make illegal read-out impossible by executing read-out by an array sequence formed by combining an identification number inputted at the time of read-out, and a random number stored at the time of write.
CONSTITUTION: When an identification number is inputted from an identification number input device 18, a pseudo random number is generated by a random number generating circuit 19, and this random number is stored in a random number storage circuit 20. Also, simultaneously, a data storage sequence corresponding to the inputted identification number and the generated random number is generated, and bit data from data lines 9-12 are stored in the corresponding memory cells, respectively. In such a state, when the identification number is inputted from the input device 18, the random number stored at the time of write is inputted to a selector control circuit 17 from the random number storage circuit 20, a selective instruction of the data line corresponding to the identification number and the random number is generated, and transferred to each selector 5-8. As a result, each selector 5-8 outputs the data stored in each memory cell 21-24 to the corresponding data lines 9-12 in accordance with its instruction.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平6－4407

(43)公開日　平成６年(1994)１月14日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　12/14	３２０　Ｂ	9293－5B		
	Ｃ	9293－5B		
9/06	４５０　Ｄ	9367－5B		

審査請求　未請求　請求項の数３(全　６　頁)

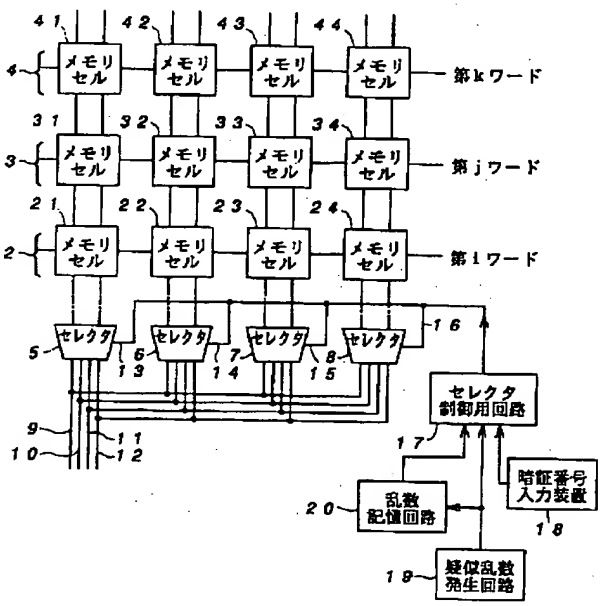
(21)出願番号　特願平4－187474

(22)出願日　平成４年(1992)６月22日

(71)出願人　000006655
新日本製鐵株式会社
東京都千代田区大手町２丁目６番３号
(72)発明者　西村　聡彦
相模原市淵野辺５－10－１　新日本製鐵株式会社エレクトロニクス研究所内
(74)代理人　弁理士　大島　陽一

(54)【発明の名称】　データ記憶装置及びデータ記憶方法

(57)【要約】
【目的】　特定の使用者のみが正規のデータを読み出すことができる記憶装置及び記憶方法を提供する。
【構成】　読み出し時に入力された暗証番号及びそのときに発生させた乱数を組み合わせてなる配列順序でデータの各分割部分を対応するメモリセルに書き込み、読み出し時に入力された暗証番号及び書き込み時に記憶された乱数を組み合わせてなる配列順序で読み出す構成とすることで、読み出し時に正しくない暗証番号を入力した際に無意味なデータが読み出されることとなり、誤った暗証番号を入力するとデータが読み出せない形式に比較して不正読み出し者にとっては解読作業及び読み出し作業に多大な労力を必要とすることから実質的に不正読み出しが不可能となり、データの機密保持を確実に行うことが可能となる。



1

【特許請求の範囲】

【請求項1】　データを所定の単位で分割し、各分割部分を各々メモリセルに対応させて記憶するデータ記憶装置であって、

暗証番号を入力する手段と、

前記暗証番号の入力に伴い乱数を発生する手段と、

前記発生した乱数を記憶する手段と、

データ書き込み時には前記入力手段から入力された暗証番号及び前記乱数発生手段にて発生した乱数に応じて、かつデータ読み出し時にあっては前記入力手段から入力された暗証番号及び前記乱数記憶手段に記憶された乱数に応じて前記各分割部分に対応するメモリセルを選択する手段と、

前記選択手段の選択結果に応じて前記各メモリセルに対して前記各分割部分の書き込み／読み出しを行う手段とを有することを特徴とするデータ記憶装置。

【請求項2】　前記データがビット単位で分割されることを特徴とする請求項1に記載のデータ記憶装置。

【請求項3】　データを所定の単位で分割し、各分割部分を各々メモリセルに対応させて記憶するデータ記憶方法であって、

データ書き込み時に、暗証番号を入力する過程と、前記暗証番号の入力に伴い乱数を発生する過程と、前記発生した乱数を記憶する過程と、前記入力手段から入力された暗証番号及び前記乱数発生手段にて発生した乱数に応じて前記各分割部分に対応するメモリセルを選択して書き込みを行う過程とを有し、

データ読み出し時に、暗証番号を入力する過程と、入力された暗証番号及び前記記憶された乱数に応じて前記各分割部分に対応するメモリセルを選択して読み出しを行う過程とを有することを特徴とするデータ記憶方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、データ記憶装置及びデータ記憶方法に関し、特にデータの不正な読み出しを防止することを目的とするデータ記憶装置及びデータ記憶方法に関するものである。

【0002】

【従来の技術】従来、例えば半導体メモリのような記憶装置にあっては、複数のメモリセルからなる複数のメモリセルセットをアドレス指定し、データを1ワード毎に各メモリセルセットに割り当て、更に各メモリセルに一定の規則に従ってワードの各ビットを割り当てて書き込み／読み出しを行っていた。

【0003】

【発明が解決しようとする課題】一方、上記したようなメモリに記憶されたデータを読み出して不正に使用されることがあり、近年そのような不正行為を防止し、機密を保持することが重要な課題となっていた。ところが、従来の記憶装置にあっては、上記したようにデータの各

2

ビットがメモリセルに対して常に一定の規則に従って対応していることから、例えば配線状態を目視により確認してアドレスを指定し、読み出し処理を行うのみでデータを容易に読み出すことができ、その内容を知ることができることから上記不正行為を防止することが困難であった。

【0004】そこで、データの入出力装置に暗証番号の入力装置及びその照合装置を設け、データの書き込み時に入力した暗証番号とデータ読み出し時に入力した暗証番号とが一致しなければ記憶されたデータを読み出すことができないようにすることが考えられる。

【0005】しかしながら、暗証番号が一致しなければデータの読み出しが行われなけれない形式の場合、不正読み出し者が試行錯誤することにより、或いは暗証番号を自動的に発生して入力する装置を作成し使用することにより、ある程度の時間があればデータを読み出すことができる。また、暗証番号を著しく複雑にすることも考えられるが、使用者が覚えられない心配があり、実用的ではない。

【0006】本発明は上記したような従来技術の問題点に鑑み出されたものであり、その主な目的は、特定の使用者のみが正規のデータを読み出すことができる記憶装置及び記憶方法を提供することにある。

【0007】

【課題を解決するための手段】上記した目的は本発明によれば、データを所定の単位で分割し、各分割部分を各々メモリセルに対応させて記憶するデータ記憶装置であって、暗証番号を入力する手段と、前記暗証番号の入力に伴い乱数を発生する手段と、前記発生した乱数を記憶する手段と、データ書き込み時には前記入力手段から入力された暗証番号及び前記乱数発生手段にて発生した乱数に応じて、かつデータ読み出し時にあっては前記入力手段から入力された暗証番号及び前記乱数記憶手段に記憶された乱数に応じて前記各分割部分に対応するメモリセルを選択する手段と、前記選択手段の選択結果に応じて前記各メモリセルに対して前記各分割部分の書き込み／読み出しを行う手段とを有することを特徴とするデータ記憶装置、及びデータを所定の単位で分割し、各分割部分を各々メモリセルに対応させて記憶するデータ記憶方法であって、データ書き込み時に、暗証番号を入力する過程と、前記暗証番号の入力に伴い乱数を発生する過程と、前記発生した乱数を記憶する過程と、前記入力手段から入力された暗証番号及び前記乱数発生手段にて発生した乱数に応じて前記各分割部分に対応するメモリセルを選択して書き込みを行う過程とを有し、データ読み出し時に、暗証番号を入力する過程と、入力された暗証番号及び前記記憶された乱数に応じて前記各分割部分に対応するメモリセルを選択して読み出しを行う過程とを有することを特徴とするデータ記憶方法を提供することにより達成される。

3

【０００８】
【作用】このようにすれば、正しい暗証番号が入力されなければ意味のないデータが読み出されることとなる。このとき、データの分割単位を一見して理解できない程度に細かく分割しておけば、読み出した時点では正しいデータであるか否かの判別を行うことができず、不正読み出し者は無意味なデータを持ちかえることとなる。また、不正読み出し者が暗証番号をランダムに自動的に発生して順番に入力するような装置を用いた場合でも膨大な意味のないデータが読み出され、これらを全て記憶する装置などを用意しなければならない。
【０００９】
【実施例】以下、本発明の好適実施例を添付の図面について詳しく説明する。尚、本実施例では記憶すべきデータのワード長が４ビットの場合を想定している。
【００１０】図１は、本発明が適用されたデータ記憶装置の構成を模式的に示すブロック図である。図示されないメモリ領域にアドレス設定されたメモリセルセット２～４は、各々ビット単位で記憶する４つのメモリセル２１～２４、３１～３４、４１～４４からなり、これら４つのセルで１つのワードをなしており、メモリセル２１～２４は第ｉワード、メモリセル３１～３４は第ｊワード、メモリセル４１～４４は第ｋワードを構成している。これらメモリセル２１～２４、３１～３４、４１～４４には、セレクタ５～８が接続されている。これら各セレクタ５～８には図示されないデータ入出力装置に接続されたデータ線９～１２が接続されている。また、各セレクタ５～８にはデータ線９～１２の他に制御信号入力線１３～１６が接続され、これら制御信号入力線１３～１６はセレクタ制御用回路１７に接続されている。このセレクタ制御用回路１７及び各セレクタ５～８により各メモリセル２１～２４、３１～３４、４１～４４に各ワードの各ビットをどのような順序で記憶させるかを選択するための選択手段を構成している。
【００１１】セレクタ制御用回路１７には例えば４桁の暗証番号を入力するための暗証番号入力装置１８と、疑似乱数を発生するための乱数発生回路１９とが接続されている。また、発生した乱数を記憶するための乱数記憶回路２０が上記乱数発生回路１９及びセレクタ制御用回路１７に接続されている。
【００１２】暗証番号が暗証番号入力装置１８から入力されると乱数発生回路１９にて疑似乱数が発生し、この乱数が乱数記憶回路２０に記憶される。そして、同時に入力された暗証番号及び発生した乱数に対応するデータ記憶順序が発生し、データ線９～１２からのビットデータを対応するメモリセルに各々記憶させるようになっている。
【００１３】次に本実施例の作動要領について第ｉワードの書き込み順序を例として図２を参照して説明する。まず、データを書き込む際に、データ線９～１２からデータ供給する前に暗証番号入力装置１８から暗証番号（例えばこれを「ＣＴＲＬ」とする。）を入力する。これと同時に乱数発生回路から乱数（例えばこれを「ＳＥＬ」とする。）を発生し、乱数記憶回路２０に記憶すると共にセレクタ制御用回路１７に伝達する。そして、セレクタ制御用回路１７内で上記暗証番号及び乱数に対応するデータ線の選択命令（例えばこれを「ＳＥＬＣＴＲＬ」とする。）を発生し各セレクタ５～８にこの選択命令「ＳＥＬＣＴＲＬ」を伝達する。

4

【００１４】図２に於て、データ線９～１２から値ｘ（０）、値ｘ（１）、値ｘ（２）、値ｘ（３）が入力され、上記データ線の選択命令「ＳＥＬＣＴＲＬ」によりセレクタ５がデータ線１０、セレクタ６がデータ線１１、セレクタ７がデータ線１２、セレクタ８がデータ線９を選択するようになっている。従って、第ｉワードに対応するメモリセルセット２の各メモリセル２１～２４には値ｘ（１）、値ｘ（２）、値ｘ（３）、値ｘ（０）がこの順番に記憶されるようになる。
【００１５】次に第ｉワードの読み出し順序を図３、図４を参照して説明する。まず、暗証番号を入力装置１８から入力すると、書き込み時に記憶された乱数が乱数記憶回路２０からセレクタ制御用回路１７に入力される。そして、これら暗証番号及び乱数に対応するデータ線の選択命令「ＳＥＬＣＴＲＬ′」が発生し、各セレクタ５～８にこれを伝達する。すると、各セレクタ５～８はその命令に沿って各メモリセル２１～２４に記憶されたデータを対応するデータ線９～１２に出力するようになる。
【００１６】セレクタ制御用回路１７には暗証番号及び乱数に対応するテーブルが用意されており、誤った暗証番号が入力されてもデータ自体は読み出すことができるようになっている。
【００１７】従って、読み出し時に入力された暗証番号が書き込み時に入力された暗証番号と一致していれば、データ線の選択命令「ＳＥＬＣＴＲＬ′」は書き込み時のデータ線の選択命令「ＳＥＬＣＴＲＬ」と一致することから、データ線９～１２に値ｘ（０）、値ｘ（１）、値ｘ（２）、値ｘ（３）がこの順番に出力され、正しいデータを構成する。
【００１８】しかしながら、読み出し時に入力された暗証番号が書き込み時に入力された暗証番号と異なっている場合、データ線の選択命令「ＳＥＬＣＴＲＬ′」は書き込み時のデータ線の選択命令「ＳＥＬＣＴＲＬ」と異なるようになり、例えば図４に示すように、セレクタ５がデータ線１２、セレクタ６がデータ線９、セレクタ７がデータ線１０、セレクタ８がデータ線１１を選択することから、データ線９～１２に値ｘ（３）、値ｘ（０）、値ｘ（１）、値ｘ（２）がこの順番に出力され、意味のない誤ったデータを構成する。
【００１９】このような操作が各ワードについて行わ

5

れ、暗証番号が一致していなければワード単位で正しいデータを得ることができないようになる。また、この読み出されたデータはビット単位で分解され、また合成されていることから、読み出された地点ではそのデータが正しいか否かを即座に判断することはできず、不正読み出し者が操作しても誤ったデータを読み出すこととなりその機密性が確保されることとなる。

【００２０】尚、乱数発生回路１９はデータの書き込み／読み出しが１回行われた後に、使用する乱数を変更するようになっており、次回同じ暗証番号を入力したとしても同じ順序では各メモリセルに記憶されないようになっている。従って、通常の暗証番号のみを入力しそれに対応する順番でデータを記憶するものに比較して一層の機密保持効果が期待できる。

【００２１】

【発明の効果】上記した説明により明らかなように、本発明による記憶装置及び記憶方法によれば、読み出し時に入力された暗証番号及びそのときに発生させた乱数を組み合わせてなる配列順序でデータの各分割部分を対応するメモリセルに書き込み、読み出し時に入力された暗証番号及び書き込み時に記憶された乱数を組み合わせてなる配列順序で読み出す構成とすることで、読み出し時に正しくない暗証番号を入力した際に無意味なデータが読み出されることとなり、誤った暗証番号を入力するとデータが読み出せない形式に比較して不正読み出し者にとっては解読作業及び読み出し作業に多大な労力を必要とすることから実質的に不正読み出しが不可能となり、データの機密保持を確実に行うことが可能となる。

6

【図面の簡単な説明】

【図１】本発明が適用された記憶装置の構成を示すブロック図である。

【図２】本発明に基づく実施例の作動要領を示すブロック図である。

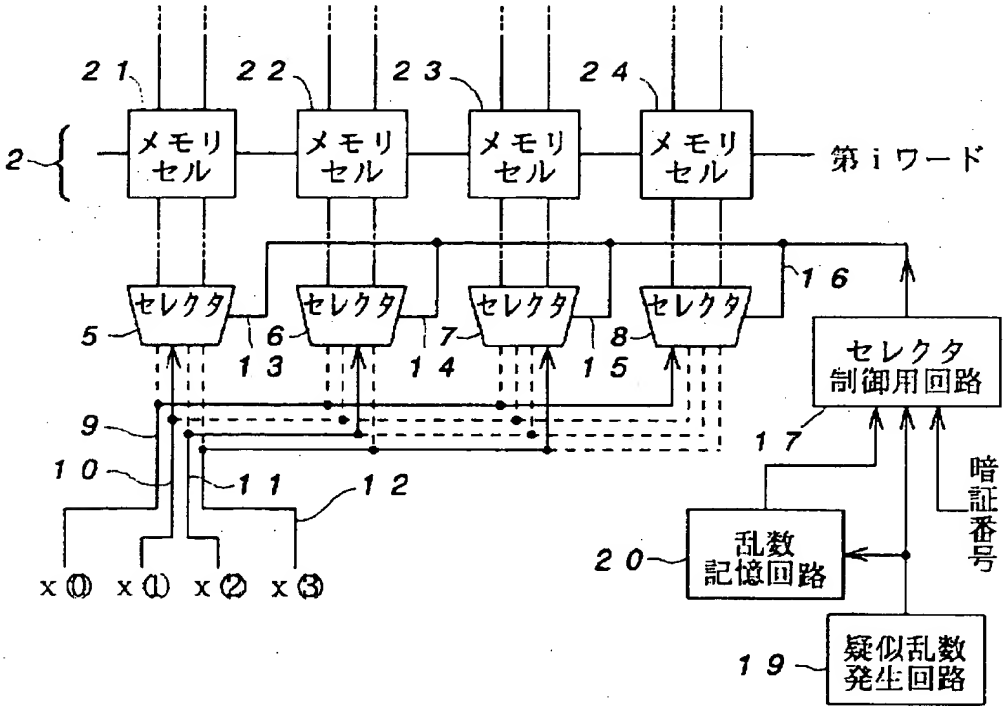
【図３】本発明に基づく実施例の作動要領を示す図２と同様なブロック図である。

【図４】本発明に基づく実施例の作動要領を示す図１及び図２と同様なブロック図である。

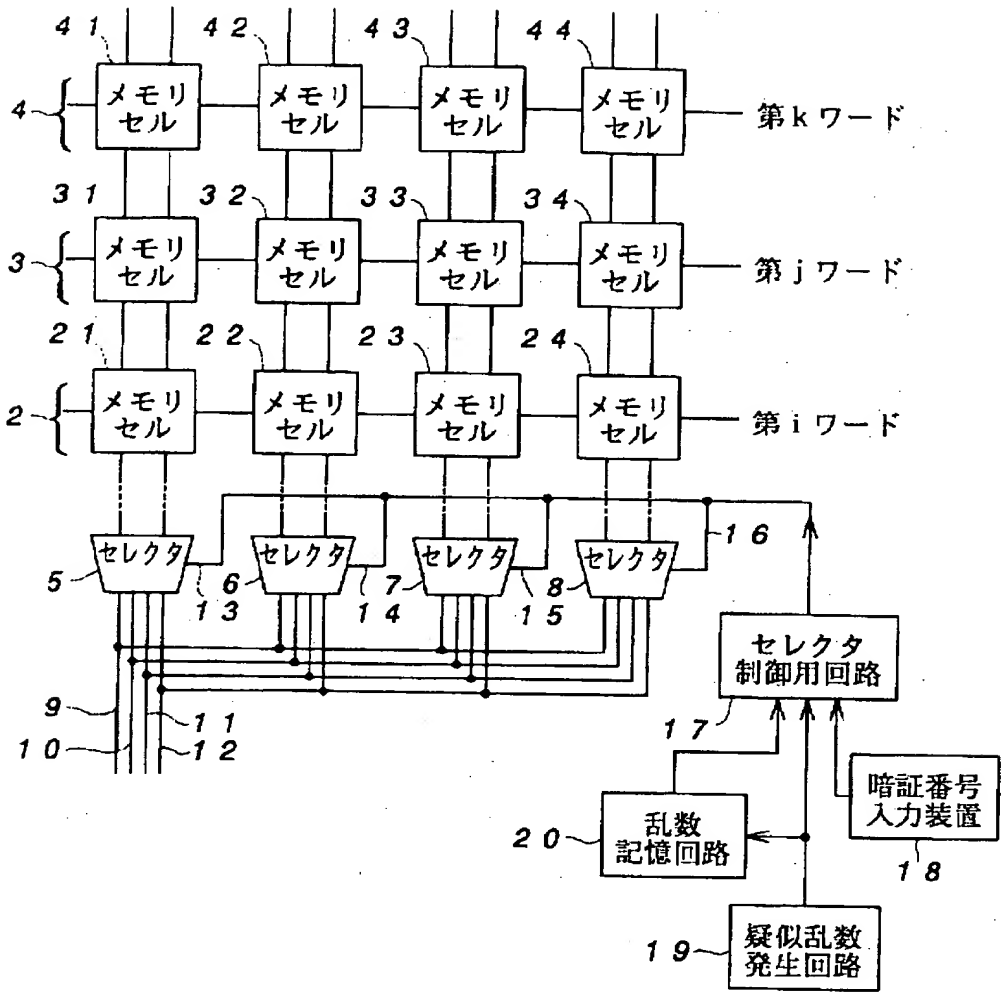
【符号の説明】

２～４　メモリセルセット
５～８　セレクタ
９～１２　データ線
１３～１６　制御信号入力線
１７　セレクタ制御用回路
１８　暗証番号入力装置
１９　乱数発生回路
２０　乱数記憶回路
２１～２４、３１～３４、４１～４４　メモリセル

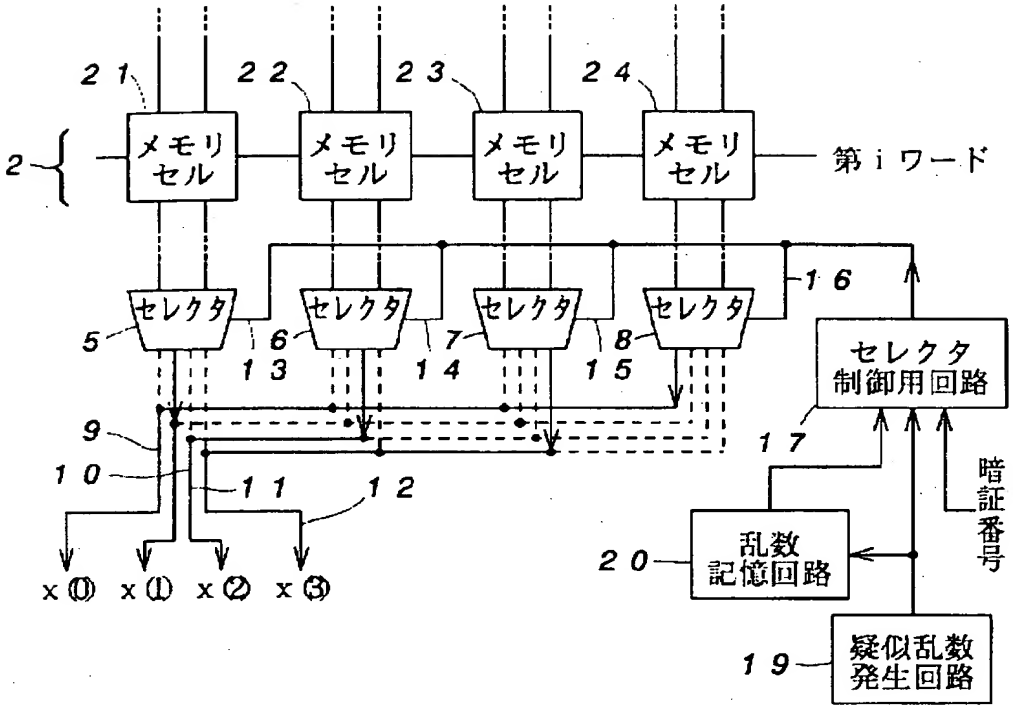
【図２】



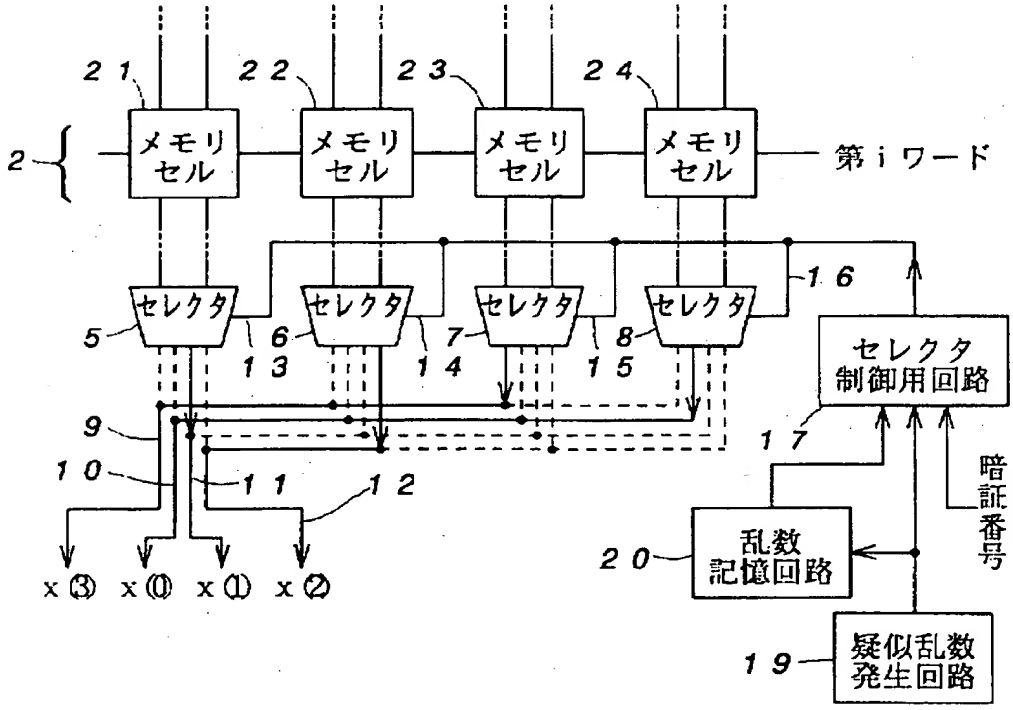
【図1】


41
42
43
44
4
メモリセル
第kワード
31
32
33
34
3
第jワード
21
22
23
24
2
第iワード
セレクタ
5
6
7
8
13
14
15
16
9
10
11
12
セレクタ制御用回路
17
暗証番号入力装置
18
20
乱数記憶回路
19
疑似乱数発生回路

【図3】


21
22
23
24
2
メモリセル
メモリセル
メモリセル
メモリセル
第iワード
16
セレクタ
セレクタ
セレクタ
セレクタ
5
6
7
8
13
14
15
セレクタ制御用回路
9
17
10
11
12
暗証番号
x⓪ x① x② x③
20
乱数記憶回路
19
疑似乱数発生回路

【図4】


21
22
23
24
2
メモリセル
メモリセル
メモリセル
メモリセル
第iワード
16
セレクタ
セレクタ
セレクタ
セレクタ
5
6
7
8
13
14
15
セレクタ制御用回路
9
17
10
11
12
暗証番号
x③ x⓪ x① x②
20
乱数記憶回路
19
疑似乱数発生回路